Virtual Private Networks (VPNs) make it possible to interconnect company sites via public IP networks and enable mobile users to dial in into their corporate networks. To achieve this aim, there are several VPN concepts which are discussed in this course in detail. A further focus is on making VPNs secure. The course will enable the participants to assess the pros and cons of various types of IP-based VPNs and to perform the design and implementation by themselves.

Course Contents
- Site-to-Site VPNs with IPv4 and IPv6
- GRE and Further Layer 3 Tunnel Protocols
- MPLS VPNs
- Layer 2 Tunnel Protocols for Remote Access VPNs
- Authentication and Authorization
- Voluntary Tunneling and Compulsory Tunneling
- Security in IP VPNs
- Encryption and Data Integrity
- IPsec for Site-to-Site VPNs
- Encapsulating Security Payload (ESP) and Authentication Header (AH)
- IKEv2
- IPsec for Remote Access VPNs
- SSL for Remote Access VPNs

E-Book You will receive the detailed documentation package from the series ExperTeach Networking – print, e-book and personalized PDF!

Target Group
The course addresses network administrators and designers who are responsible for the planning and technical implementation of VPNs on the basis of different tunneling technologies in IPv4 and IPv6 networks. Attendance at this course can be credited for T.I.S.P. recertification.

Prerequisites
Profound network know-how, particularly of the TCP/IP protocol stack and the corresponding addressing and routing concepts, is required. These contents are imparted in the TCP/IP - Protocols, Addressing, Routing course.

This Course in the Web
You can find the up-to-date information and options for ordering under the following link: www.experteach-training.com/go/IPVPN

Reservation
On our Website, you can reserve a course seat for 7 days free of charge and in an non-committal manner. This can also be done by phone under +49 6074/4868-0.

Guaranteed Course Dates
To ensure reliable planning, we are continuously offering a wide range of guaranteed course dates.

Your Tailor-Made Course!
We can precisely customize this course to your project and the corresponding requirements.

<table>
<thead>
<tr>
<th>Training</th>
<th>Prices, excl. of V.A.T.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classroom training</td>
<td>4 Days</td>
</tr>
<tr>
<td></td>
<td>€ 2,195</td>
</tr>
</tbody>
</table>

Date/course venue
- 07/01-10/01/20 Frankfurt
- 04/05-07/05/20 Frankfurt
- 02/11-05/11/20 Frankfurt

Status 09/22/2019
1 VPN Technologies—An Introduction

1.1 Why VPNs?

1.1.1 Which VPN Technologies Are Used?

1.1.2 Frame Relay or ATM VPNs

1.1.3 Demands Made on the VPN Solution

1.2 VPNs with MPLS and BGP-4

1.3 IP VPNs

1.4 VPN and Security

1.4.1 Security Requirements

1.4.2 Security in Classical VPNs

1.4.3 Security in IP VPNs

2 From the Tunneling Protocol to VPN

2.1 Layer 2 Tunnels for Networks

2.1.1 IP-in-IP Tunneling

2.1.2 Generic Routing Encapsulation (GRE)

2.1.3 IPSec as a Tunneling Protocol

2.2 Layer-2 Tunnels for Dial-Up Clients

2.2.1 The Role of PPP

2.2.2 VPDN—Compulsory or Voluntary Tunneling

2.2.3 Layer-2 Tunneling Protocols

2.2.4 Layer-2 IP VPNs and IPSec

3 Security for VPNs

3.1 What Does Security Mean?

3.2 Symmetrical Encryption

3.2.1 Lifetime of the Keys

3.2.2 Distribution of Keys

3.2.3 Asymmetrical Encryption

3.3 Data Integrity: Hash Values

3.3.1 Typical Features

3.3.2 Keyed Hash

3.4 Data Origin Authentication

3.4.1 Pre-Shared Key

3.4.2 Public Key Procedure

3.4.3 Certificates

3.4.4 PKI and CA

3.5 Replay Attacks

3.5.1 IPsec and Co.—Security Levels

4 IPsec VPN

4.1 The Objectives of IPsec

4.2 IPsec in Application

4.2.1 Host-to-Host

4.2.2 IPsec—Gateway-to-Gateway

5 SSL VPN

5.1 SSL—Security for TCP

5.1.1 The SSL Protocol Stack

5.1.2 SSL Versions and TLS

5.2 SSL Connection Setup

5.2.1 Phase 1—Say Hello

5.2.2 Phase 2 and 3—Certificates

5.2.3 Phase 4—Completion of Handshake

5.3 Secure Data Transfer

5.4 Components of an SSL VPN

5.4.1 The SSL Gateway

5.4.2 Client-less with Portal

5.4.3 The SSL-Client

5.5 Concepts for the Application of SSL VPNs

5.5.1 Connecting Subsidiaries with SSL

5.5.2 SSL for the Connection of Teleworkers

5.5.3 SSL for Mobile Users

5.5.4 SSL in the Internet Café

5.6 Problems with SSL VPNs

5.6.1 Problems with Applications

5.6.2 Client Security

5.7 Product Selection

5.7.1 Solutions by Microsoft

5.7.2 Check Point Security Gateway—VPN-1

5.7.3 Options with Cisco

5.7.4 OpenVPN